UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/761,700	01/18/2001	Ashok Vadekar	06944.0033	4704

22852 7590 02/24/2004

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER	
MEISLAHN, DOUGLAS J	

ART UNIT	PAPER NUMBER
2137	7

DATE MAILED: 02/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/761,700	Applicant(s) VADEKAR ET AL.	
	Examiner Douglas J. Meislahn	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-6 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-6 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 18 January 2001 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 4.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

2. The drawings are objected to because the "Substitute Sheet" at the bottom of all of the figures should be deleted. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Objections

3. Claims 1 and 6 are objected to because of the following informalities: in claim 1, the colon at the end of the preamble should not be on a separate line; in claim 6, "if" in the ninth line should be "of". Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claim 1 recites the limitations "the group" in its second line, "the group identity element" in part (b), "said selected bits" in the preamble of part (c), "said group element" in part (c)(iii), "said last selected bit" in part (d), "said integral" in the second to last line, and "said cryptographic system" also in part (d). There is insufficient antecedent basis for these limitations in the claim. In order: "group" is used as an adjective earlier in the claim; there is no obvious correction for or further explanation needed to clarify the rejection of "the group identity element"; changing "said" to "the" would overcome the "said selected bits" rejection; again, change "said" to "the" to overcome the "said group element" rejection; both "said last selected bit" and "said cryptographic system" clearly need antecedent basis. The "said integral" error would be corrected by placing "number" at its end.

7. Claim 2 recites the limitation "the multiplicative inverse 1/g" in its third line. There is insufficient antecedent basis for this limitation in the claim. Delete "the".

8. Claim 4 recites the limitation "the elliptic curve" in the second line, "the scalar multiple kP" in the third line and "the negative –P" across the last two lines. There is insufficient antecedent basis for these limitations in the claim. Delete all three recitations of "the" and replace with "an" or "a".

9. Claim 5 recites the limitation "said integral value". There is insufficient antecedent basis for this limitation in the claim. Replace "value" with "number".

10. Claim 6 recites the limitations "said group" in the second line, "said recorded bits" in the sixth line, "said selected bits" across lines six and seven, "said selected element" in the eighth line, "said sign" in the ninth line, and "said intermediate value" in the last line. There is insufficient antecedent basis for

these limitations in the claim. The first problem phrase is similar to that of claim 1; the second and third errors would be fixed by replacing "said" with "the"; the examiner has no suggestions on how to correct the fourth problem; the fifth problem might best be fixed by rewriting the second clause to provide antecedent basis for "said sign" ("recoding the binary vector to produce a digit representation with a sign of either plus one or minus one", for example); to correct the last problem, change "value" to "element".

11. The term "substantially" in claim 1 is a relative term which renders the claim indefinite. The term "equal" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 101

12. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-5 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim is directed to a method that is neither specific to a computer nor a machine. Specifying in claim 1 that the method is implemented on a computer would overcome the rejection.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Kocher (6539092), Kocher et al. (6381699, 6327661,

6304658, 6298442), Hollmann et al. (6366673) - not prior art, Ishii et al. (6175850), Graunke et al. (6041122), Shamir (5991415), and Clapp (5987131). All of these references pertain to timing attacks. A complete analysis of their relation to the patentability of the claims cannot be undertaken due to the ambiguities stemming from the causes of the 112 rejections.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Douglas J. Meislahn
Examiner

Art Unit 2137

DJM